

1 What is claimed is:

2  
3 1. An apparatus for maintaining the privacy of a plaintext message transmitted  
4 over a non-secure channel between a transmitting party and a receiving party without  
5 cryptographic key exchange between said parties, comprising:

6 (a) first transformation means for embodying the plaintext message in a non-  
7 reversible first output;

8 (b) second transformation means for generating a second output which is a  
9 reversible second transformation of said first output, such that said second output is non-  
10 reversible;

11 (c) first transmitting means for transmitting said second output from the  
12 transmitting party to the receiving party;

13 (d) third transformation means for generating a third output which is a reversible  
14 third transformation of said second output, such that said third output is non-reversible;

15 (e) second transmitting means for transmitting said third output from the receiving  
16 party to the transmitting party;

17 (f) reverse second transformation means for generating a fourth output through  
18 reversal of the second transformation applied to said third output, such that said fourth  
19 output is non-reversible;

20 (g) third transmitting means for transmitting said fourth output from the  
21 transmitting party to the receiving party;

22 (h) reverse third transformation means for generating said first output through  
23 reversal of the third transformation applied to said fourth output; and

24 (i) extracting means for extracting the plaintext message from said first output in  
25 the possession of the receiving party.

26  
27 2. An apparatus according to claim 1, wherein said first transmitting means is  
28 also said third transmitting means.

29  
30 3. An apparatus according to claim 1, wherein

31 (a) said first transformation means comprises a first mathematical function  
32 creating an embodiment of the plaintext message in a non-invertible first output;

33 (b) said second transformation means comprises an invertible second  
34 mathematical function;

35 (c) said third transformation means comprises an invertible third mathematical  
36 function;

37 (d) said reverse second transformation means comprises the inverse of said  
38 second mathematical function; and

39 (e) said reverse third transformation means comprises the inverse of said third  
40 mathematical function.

41  
42 4. A method for securely transmitting a plaintext message from a transmitting  
43 party to a receiving party over a non-secure channel, comprising the steps of:

44 (a) generating a first transformation of the plaintext message such that the  
45 plaintext message is embodied in a first output of said first transformation and said first  
46 output of said first transformation is non-reversible;

1 (b) generating a reversible second transformation of said first output of said first  
2 transformation such that a second output of said second transformation is non-reversible;  
3 (c) transmitting said second output of said second transformation from the  
4 transmitting party to the receiving party;  
5 (d) generating a reversible third transformation of said second output of said  
6 second transformation such that a third output of said third transformation is non-  
7 reversible;  
8 (e) transmitting said third output of said third transformation from the receiving  
9 party to the transmitting party;  
10 (f) reversing said second transformation on said third output of said third  
11 transformation such that a fourth output of said reversal of the second transformation is  
12 non-reversible;  
13 (g) transmitting said fourth output of said reversal of the second transformation  
14 from the transmitting party to the receiving party;  
15 (h) reversing said third transformation on said fourth output to yield said first  
16 output of said first transformation; and  
17 (i) extracting the plaintext message from said first output.

18  
19 5. A method according to claim 4, wherein said first transmitting means is also  
20 said third transmitting means.

21  
22 6. A method according to claim 4, wherein:  
23 (a) said first transformation comprises a first mathematical function creating an  
24 embodiment of the plaintext message in a non-invertible first output;  
25 (b) said second transformation comprises an invertible second mathematical  
26 function;  
27 (c) said third transformation comprises an invertible third mathematical function;  
28 (d) said reverse second transformation comprises the inverse of said second  
29 mathematical function; and  
30 (e) said reverse third transformation comprises the inverse of said third  
31 mathematical function.

32  
33 7. An apparatus for maintaining the privacy of a plaintext message conveyed  
34 over a non-secure channel between a transmitting party and a receiving party wherein:  
35 (a) the transmitting party neither possesses nor uses any cryptographic key that  
36 was created by the receiving party;  
37 (b) the receiving party neither possesses nor uses any cryptographic key, that was  
38 created by the transmitting party;  
39 (c) neither the transmitting party nor the receiving party exchanged a  
40 cryptographic key with the other party, and  
41 (d) the plaintext message is transmitted to and understood by the receiving party,  
42 but cannot be understood by any third party who was privy to all transmissions between  
43 the transmitting party and the receiving party.

44  
45 8. A method for maintaining the privacy of a plaintext message conveyed over a  
46 non-secure channel between a transmitting party and a receiving party wherein:

1 (a) the transmitting party neither possesses nor uses any cryptographic key, that  
2 was created by the receiving party;

3 (b) the receiving party neither possesses nor uses any cryptographic key, that was  
4 created by the transmitting party;

5 (c) neither the transmitting party nor the receiving party exchanged a  
6 cryptographic key, with the other party and

7 (d) the plaintext message is transmitted to and understood by the receiving party,  
8 but cannot be understood by any third party who was privy to all transmissions between  
9 the transmitting party and the receiving party.

10  
11 9. An apparatus according to claim 1, wherein said plaintext message comprises a  
12 cryptographic key.

13  
14 10. A method according to claim 4, wherein said plaintext message comprises a  
15 cryptographic key.  
16